Raytheon
BBN Technologies

BBN Technologies Corp.
10 Moulton Street
Cambridge, MA 02138

6 February 2015

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
richard.t.willis@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance:	7 February 2014 – 7 February 2016
Total Contract Amount:	$475,359 (Base)
Amount of Incremental Funds:	$280,668
Total Amount Expended (thru 30 January):	$219,571

Attention: Dr. Richard Willis
Subject: SeaKey Phase I Annual Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Phase I Annual Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

Distribution Statement A. Approved for public release; distribution is unlimited.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
06 FEB 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **BBN Technologies Corp.,,10 Moulton Street,,Cambridge,,MA,02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**33**	

SEAKEY Phase I Annual Report for the Period 7 February 2014 through 6 February 2015

Section A. Project Summary

This is the SEAKEY final report for the BBN-RVS team for the Phase I reporting period, February 2014 through February 2015. Our tasks under this project include identifying key challenges to transition QKD to a naval environment and determination of optimum operating parameters for a naval QKD system, in pursuit of the Seakey end-of-program goal of achieving key rates of 1Mbit/sec at a range of 10-30 km in a naval environment.

Program Highlights:

1. Fundamental upper bound to the key rate achievable using any QKD protocol over a lossy channel.
2. Developed a MATLAB tool for the evaluation of secret key rates under turbulent propagation (a theoretical model) and atmospheric absorption and scattering (a numerical model taken from MODTRAN), while employing a single spatial mode.
3. A quantitative trade study of using multiple spatial modes and finding up to how many spatial modes may yield a perceivable key rate benefit.
4. Development of a quantum-secure direct communication protocol with near-optimal rate-loss tradeoff that uses laser light modulation and homodyne detection, that is immune to a quantum-limited passive eavesdropper.
5. Identification of a potentially far-reduced-complexity high-rate CV KD protocol.

This report is organized as follows:

1. This document (containing minor programmatic points, organizational notes and summary of progress in Phase I);
2. A PPTX document (SEAKEY_RESULTS_Y1) containing the summary presentation of Phase I; and
3. A folder (Model) containing the GUI m-file Input_parameters.m used to calculate key rates with inputs from the MODTRAN database.

Section B. Technical Progress

In this section, we describe the Statement of Work (SoW) proposed for Phase I and our progress against each of the tasks in the SoW.

Task 1 Identify key challenges for transition QKD to a naval environment. Examine rate-distance tradeoffs with turbulence, scattering, absorption, background etc.

Distribution Statement A. Approved for public release; distribution is unlimited.

SoW: The first step addressing this problem will be to identify all of the vulnerabilities QKD will be subject to when deployed in a naval environment. The evolution toward designing a robust, high-performance QKD system for a naval environment will begin with a study to identify the key challenges to QKD in such an environment, and quantitatively assess their impact on system performance. This initial focused four month analysis will categorize the effects most deleterious to fielding a high performance QKD system.

Phase I Results:

The Seakey team has focused on investigating the rate-loss behavior of the two classes of quantum key distribution protocols - discrete-variable (DV) and continuous-variable (CV). In recent work (arXiv:1310.0129), Guha et al defined the Rate-Upper Bound, which sets an upper limit on the secret key capacity of a pure-loss bosonic channel. As seen from Figure 1, CV and DV protocols have the same optimal rate-loss scaling, given by $R \sim \eta$. In particular, CV binary-phase-shift-keying (BPSK) and DV (polarization, or time-bin encoded) BB84 without decoy states, both yield a worse ($R \sim \eta^2$) scaling. Thus, an extension of the CV BPSK protocol with a few additional modulation levels (but far fewer from a QAM-sampled discretization of the full Gaussian distribution of amplitude and phase, that CV demonstrations use) should retrieve the optimal ($R \sim \eta$) key rate scaling. This would be the same effect that decoy yields for DV. The security analysis for this will be pursued in Phase II.

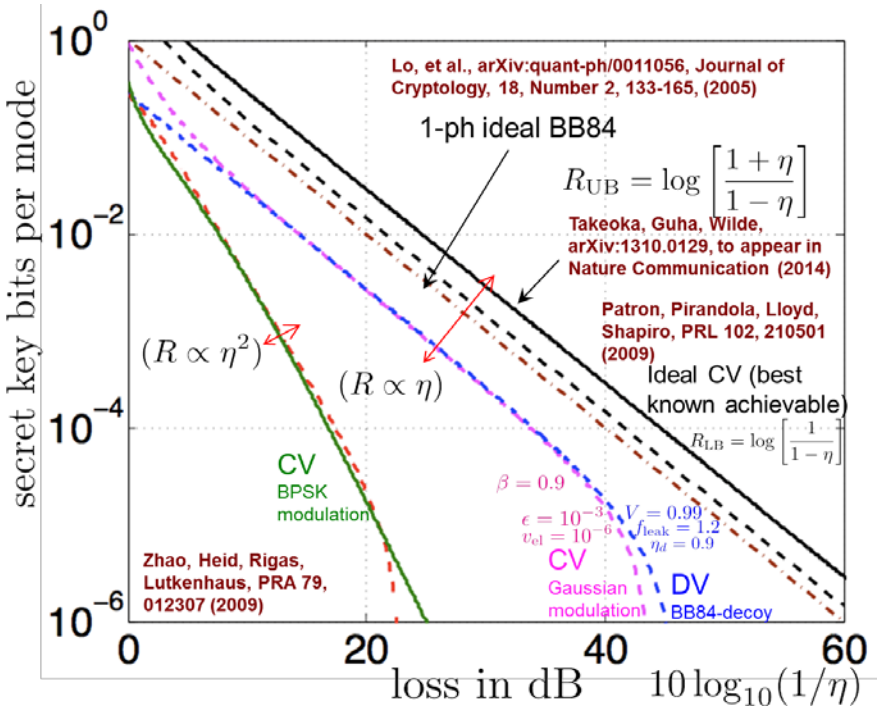


Figure 1: Rate vs loss.

Distribution Statement A. Approved for public release; distribution is unlimited.

While the fundamental rate trade-offs show similar trends for CV and DV, CV protocols have lower noise (being only limited by local-oscillator shot-noise of the coherent-detection receiver) and can access a higher number of modes/second, because homodyne or heterodyne detection can potentially have a much higher bandwidth compared to single photon detection, at comparable detection efficiencies. On the other hand, error-correction codes are better developed for small-alphabet DV protocols. Because DV protocols have small discrete signaling constellations, modulation is simpler, as compared to CV protocols (where symbols must be chosen from a Gaussian distribution or a densely-quantized version thereof). Thus, an extension of the CV-BPSK protocol that only uses a few modulation constellation points, while achieving the R~η rate-loss scaling, will ease on the aforesaid hardest obstacle to CV implementations.

Guha et al have invented a direct communication protocol, that is quantum secure to a passive eavesdropper (same benchmark of security as the Shapiro two-way protocol), but requires only a simple one-way binary-phase laser-light signaling, near-LO-shot-noise-limited homodyne detection, and a reverse authenticated public classical channel (which may be an RF link for instance). The bits/mode performance of this protocol is several orders of magnitude better than the Shapiro protocol, which needs entangled states. The bits/mode performance achieved by our protocol adheres the quantum-limited rate-loss scaling (R~η), and is only factor of 2 to 3 below it for reasonable assumptions on sources and homodyne detection.

The team investigated various atmospheric nonidealities, including the effects of (1) atmospheric absorption, (2) aerosols, (3) water vapor, (4) turbulence-induced amplitude and phase fluctuations, on loss, and that of the blackbody and sky radiance on detector background counts. The main objective was to zero in on a few candidate windows of operation. Taking into account the trade-off between blackbody radiance, sky radiance and atmospheric transmission, the three candidate wavelengths we identified are 1.5 μm, 2.2 μm and 4μm (see Figure 2). Of 2.2 μm and 4 μm, former has worse (higher) loss, but better (lower) noise.

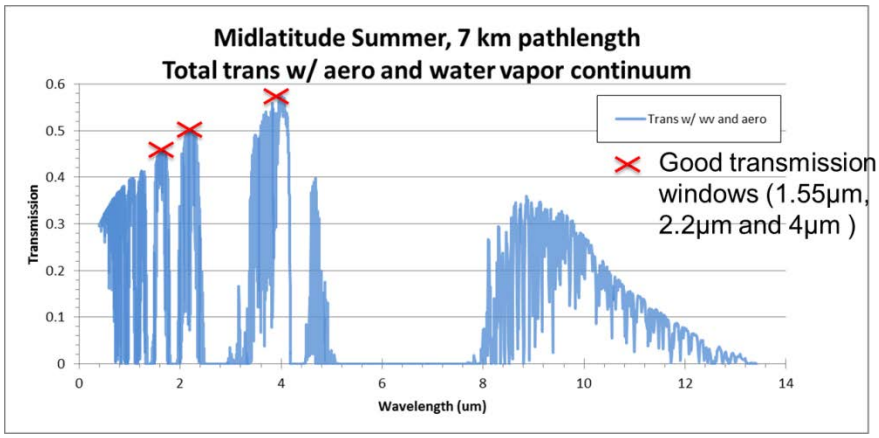


Figure 2: Atmospheric transmission in a marine environment in the presence of water vapor and aerosol (23km visibility).

Distribution Statement A. Approved for public release; distribution is unlimited.

A focal point in Phase I was our investigation of the performance of the BB84 decoy state protocol at these three wavelength regions: 1.55 μm , 2 μm and 4 μm. Interestingly, the team found that in the presence of turbulence, atmospheric loss and sky/blackbody radiance, the three wavelength windows exhibit *similar* performance (Figure 3). Thus, the choice of wavelength of operation really depends on the availability of optical components – laser sources, detectors, modulators – at the various wavelengths. Given the easy availability of components in the 1.5 μm telecom band, this is the most suitable option.

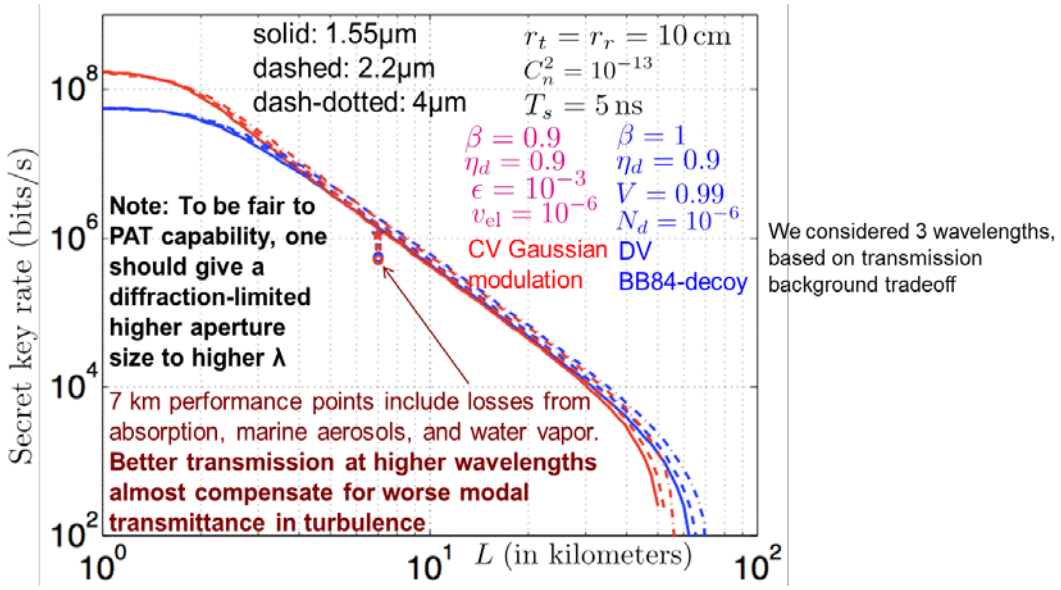


Figure 3: Performance of the BB84-decoy and CV Gaussian modulation protocols across wavelengths.

The Seakey team identified the 1.5 μm FSO communication hardware developed by Novasol Inc. as a suitable platform from for implementation of a QKD testbed.

<u>Task 2.</u> Trade study that includes detailed evaluation of atmospheric turbulence, and QKD implementation to determine optimum operating parameters for deployed naval QKD system. Optimize performance across choice of protocol, code, modulation, wavelength, transmitter-receiver technology.

SoW: Once the vulnerabilities of a standard free-space QKD system operating in a naval environment have been identified, Raytheon BBN will design a QKD system complete with technologies to mitigate or minimize the risks incurred by operating in such an environment. Our team will identify the QKD protocol (e.g. BB84 with decoy states, CV-QKD), the encoding and modulation format (e.g. polarization, phase, time-bin, spatial, including high-order modulations), the wavelength of operation (e.g. specific wavelength within the visible, NIR or MWIR band), and the optimal optical channel parameters (e.g. beam waist).

Distribution Statement A. Approved for public release; distribution is unlimited.

Phase I Results: The performance of CV Gaussian and DV BB84 protocols with variation in atmospheric turbulence is shown in Figure 4, which plots the secret key rates as a function of channel loss. We assume the fundamental Gaussian beam is modulated, and that the apertures are circular. For this plot, all the "loss" has been lumped into one dB figure (the x axis), which could have contributions from diffraction-limited beam-spread, atmospheric scattering due to aerosols and water vapor, and any coupling efficiency loss at the receiver—for instance the free-space to fiber mode coupling efficiency in a fiber-coupled detector. Realistic device parameters (as listed in the plot legend) were chosen for both CV and DV implementations. As expected, the key rate vs. loss degrades with increasing C_n^2. Roughly speaking, one order of magnitude increase in C_n^2 results in the key rates to diminish by one order of magnitude.

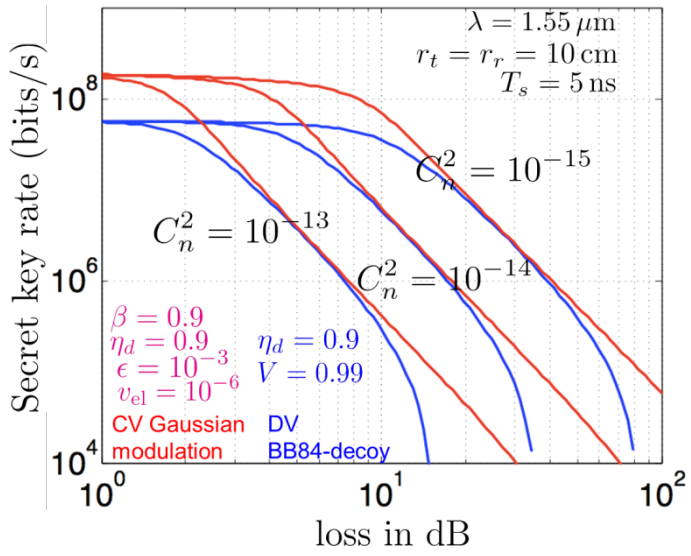


Figure 4: Effect of turbulence strength on secret key rate of the CV Gaussian modulation and DV BB84-decoy protocols.

In order to further quantify the effects of various marine detriments on quantum key distribution rates, our team built a numerical model, implemented in Matlab (Input_parameters.m). This model calculates the key rates of the BB84-decoy and CV-Gaussian modulation protocols for a specific link geometry by taking into account user-defined values of wavelength, weather conditions, visibility (which corresponds to aerosol concentration values), and elevation above sea-level. The link geometry considered accounts for transmit and receive-apertures of radius 10 cm, symbol duration of 5ns, detector efficiency of 0.9 and dark count probability of 10^{-6}. Figure 5 shows a screenshot of the Matlab GUI. The differing weather/visibility conditions cause a rapid decline in secret key rate of both, the BB84-decoy state and CV–Gaussian modulation protocol. As a best case scenario, we expect key rates of the order of 10^6 at a range of 100m.

Distribution Statement A. Approved for public release; distribution is unlimited.

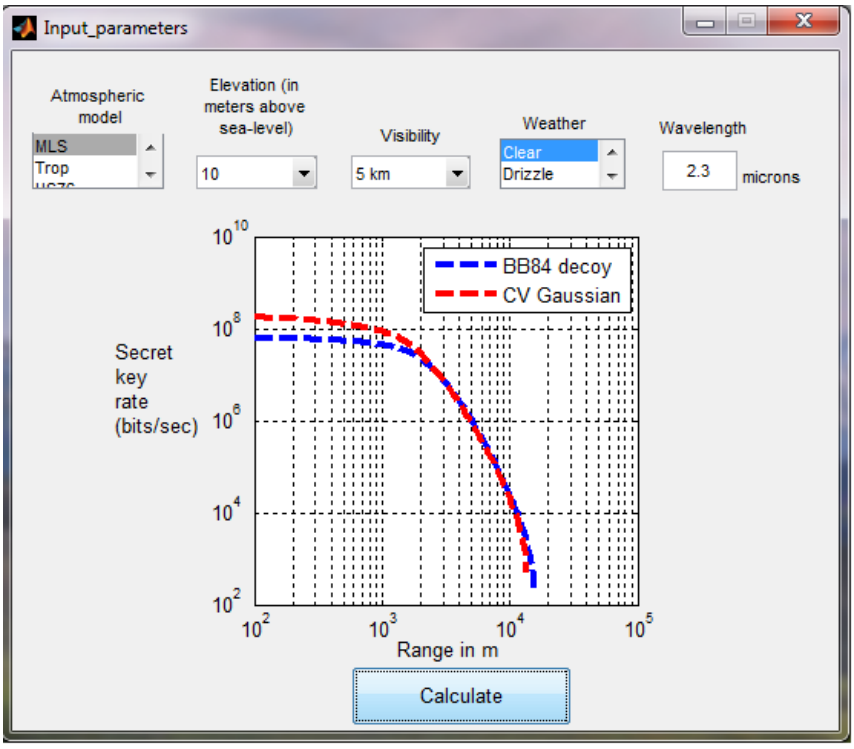


Figure 5: Screenshot of Matlab GUI

We further examined the performance improvement by using multiple spatial modes. We considered a soft-aperture configuration of Hermite-Gaussian and Laguerre-Gaussian modes, for which the modal transmissivities are exactly solvable. From Figure 6, it is seen that the advantage of using multiple spatial modes manifests itself at shorter ranges, below 1 km. At longer ranges, employing multiple spatial modes does not pose any advantage due to diffraction-induced broadening.

Distribution Statement A. Approved for public release; distribution is unlimited.

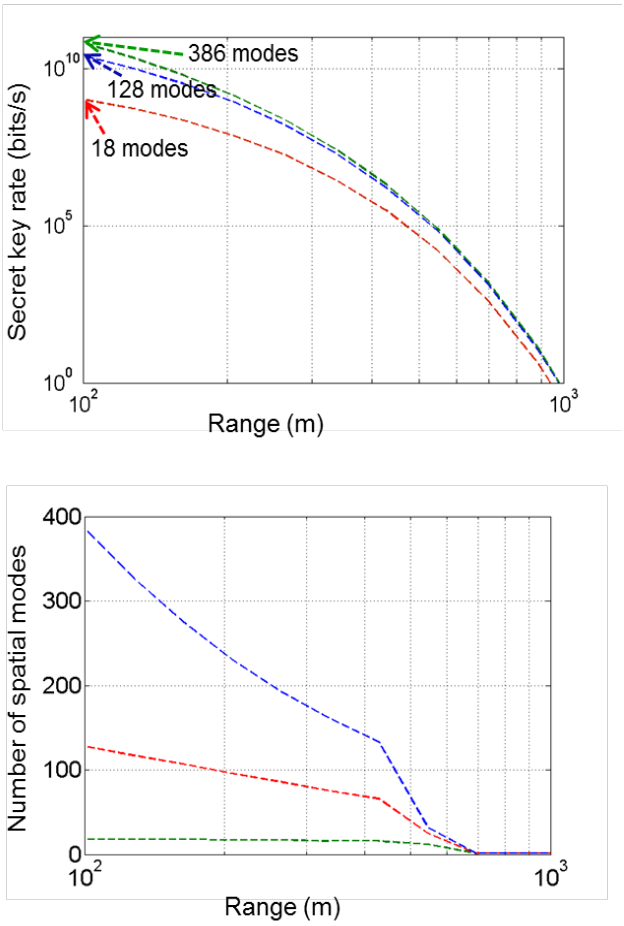


Figure 6: Secret key rates as a function of range, obtained by employing multiple spatial modes (upper figure). Number of spatial modes as a function of range (lower figure).

Section C. Publications

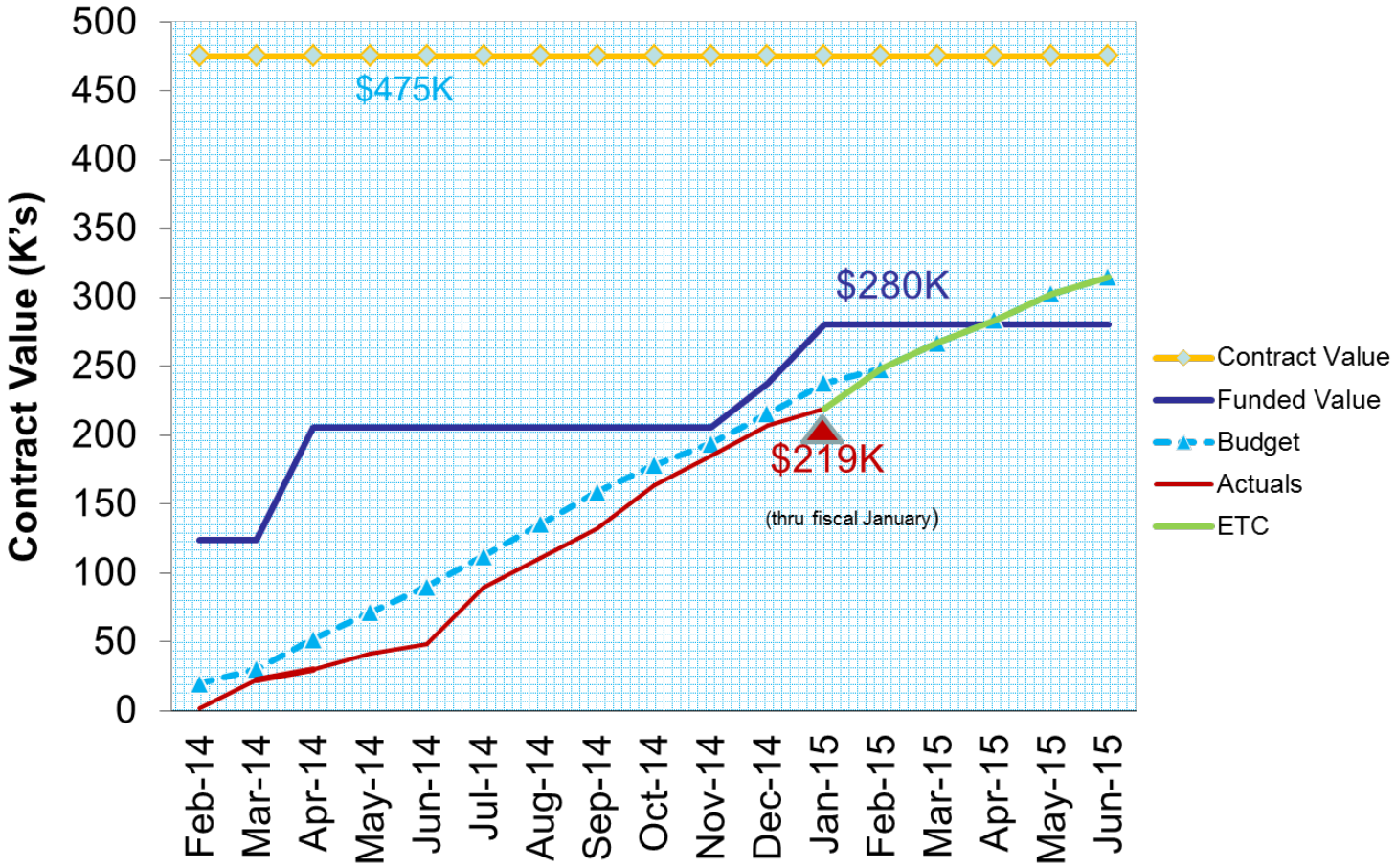
- M. Takeoka, S. Guha, M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," Nature Communications 5, doi:10.1038/ncomms6235 (October 24, 2014).
- S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. Shapiro, S. Pirandola, "Quantum Illumination at the Microwave Wavelengths," (to be published in PRL in March 2015), (January 31, 2015).

To be published:

- S. Guha, M. Takeoka, H. Krovi, M. Wilde, C. Lupo, "Defeating passive eavesdropping using a laser-source and homodyne detection".

Distribution Statement A. Approved for public release; distribution is unlimited.

Section D. SEAKEY Financial Status



Distribution Statement A. Approved for public release; distribution is unlimited.

Appendix - Summary of Phase I (PowerPoint Slides)

Distribution Statement A. Approved for public release; distribution is unlimited.

SeaKey Goals

Raytheon BBN Technologies

- Evaluate, adapt and optimize free-space QKD technology for demonstration and deployment on naval platforms such as surface ships linked via free-space channels to aircraft-based, land-based or other ship-based optical transceivers

Year 1
- Identify challenges unique to marine deployment, rate-distance tradeoffs with turbulence, scattering, absorption, background, PAT error (e.g., due to platform fluctuations)
- Optimize performance across choice of protocol, code, modulation, wavelength, transmitter-receiver technology

Year 2
- Design end-to-end system to enable key exchange over useful range (10-30 km) at useful rates (10-100 Mbits/s)
- Enabling technology identification/development, custom simulation of reach, rate w/ naval data, implementation

Our Team and Collaborators

Raytheon BBN Technologies

SEAKEY

Name	Role	Contact
Kathryn Carson	Program Manager	kcarson@bbn.com
Jonathan Habif	Principal Investigator	jhabif@bbn.com
Saikat Guha	Theorist	sguha@bbn.com
Monika Patel	Experimentalist	mpatel@bbn.com
Michael Jack	Modeling / Detectors	mdjack@raytheon.com
Matthew Thomas	Modeling	Matthew.C.Thomas@raytheon.com

SECANT

Name	Role	Contact
Saikat Guha	Principal Investigator	sguha@bbn.com
Marcus P. da Silva	Theorist: QIT, QECC	msilva@bbn.com

Collaborators	Institution	Programs	Topics
Jeffrey H. Shapiro	MIT	SEAKEY / ONR	Turbulence, propagation
Norbert Lütkenhaus	IQC	SECANT / Sandia	Protocols, repeaters

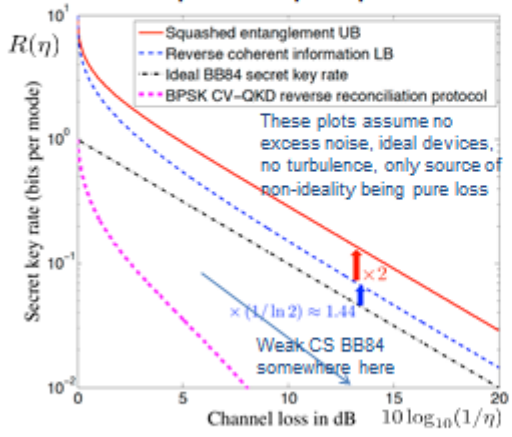
Distribution Statement A. Approved for public release; distribution is unlimited.

Technical update

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

QKD over single-mode channel

- Fundamental tradeoff between QKD key rate and input-output power transmittance, $\eta \in (0, 1]$

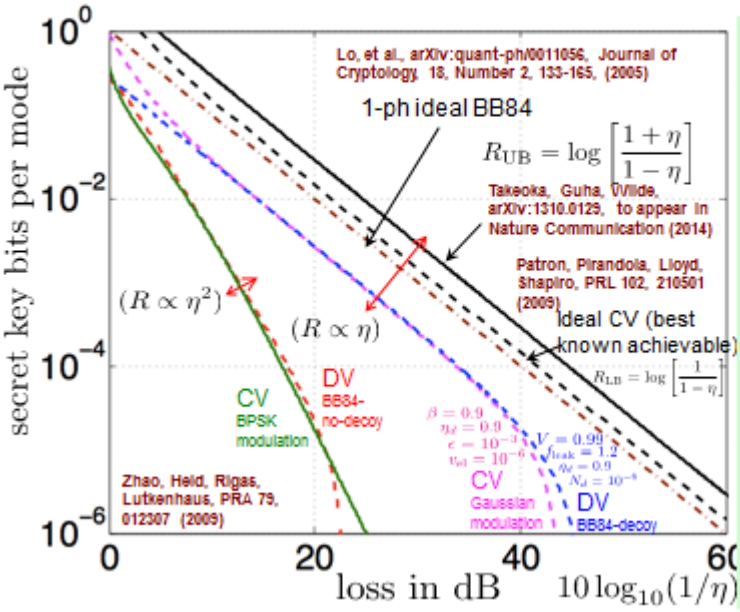


- UB on key rate for *any* QKD protocol, $\log_2(1+\eta)/\log_2(1-\eta)$
  Takeoka, Guha, Wilde, arXiv:1310.0129 [quant-ph] submitted to Nature Photonics (March, 2014)
- Ideal BB84, biased bases, deterministic SPS, $R(\eta) \approx \eta$
  Lo, et al., arXiv:quant-ph/0011056, Journal of Cryptology 18, Number 2, 133-165, (2005)
- Rev. coh-inf LB, achievable w SPDC + displacement modulation, $1/\log_2(1-\eta)$
  Patron, Pirandola, Lloyd, Shapiro, Phys. Rev. Lett. 102, 210501 (2009)
- CV-QKD, BPSK + homodyne
  Lutkenhaus group—PRA 73, 052316 2006, PRA 76, 022313 2007, PRA 79, 012307 2009

Best-case key rate for point-to-point QKD must decay as $R(\eta) \approx \eta$, regardless of QKD protocol or power. Optimal transmit-power depends on loss. SP-BB84 pretty good. Far field LOS, $D_f \equiv A_t A_r/(\lambda L)^2 \ll 1$, transmittance $\eta \approx D_f \propto 1/L^2$

Distribution Statement A. Approved for public release; distribution is unlimited.

Rate vs. loss



CV and DV have same optimal rate-scaling, R~η

CV binary and DV without decoy yield R~η² scaling

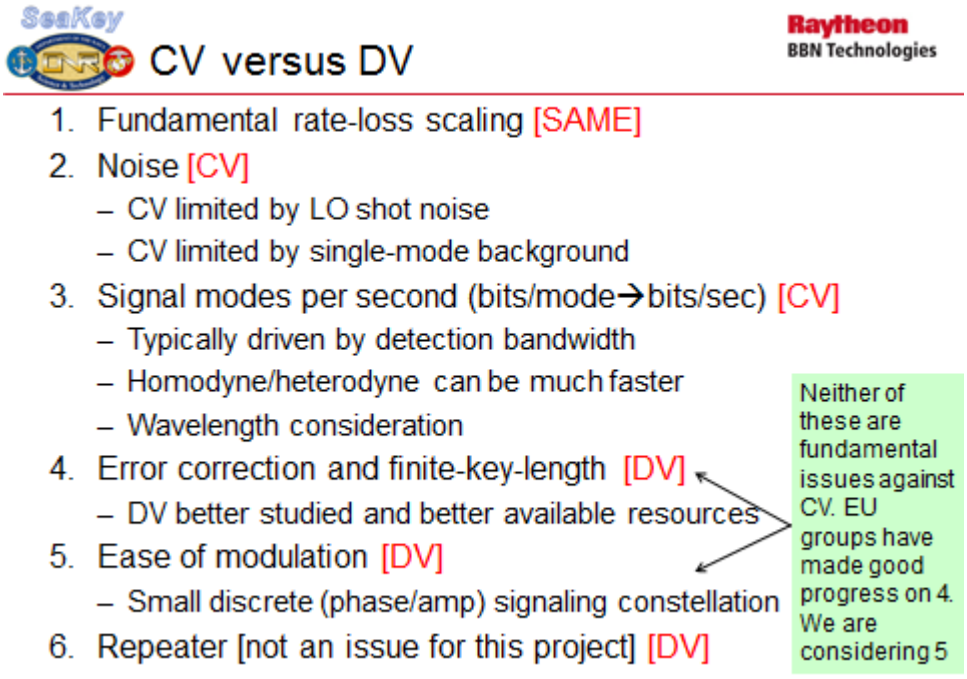
CV with few modulation levels (not full Gaussian) should retrieve optimal (R~η) key rate scaling [same effect that decoy yields for DV], will make CV a LOT more attractive

security proof yet to be completed

Technical update

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

Distribution Statement A. Approved for public release; distribution is unlimited.



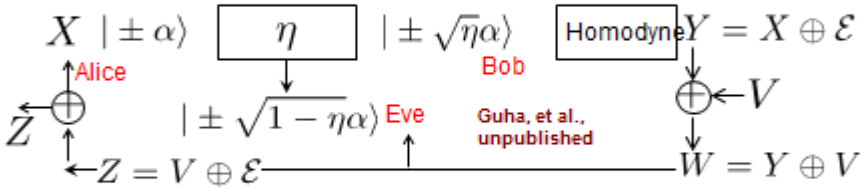
Distribution Statement A. Approved for public release; distribution is unlimited.

Technical update

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

High-rate direct-secure (LPI) comm using DSSS laser light, homodyne

- Direct quantum-secured communication immune to passive eavesdropping
  - Does NOT need entanglement (as in Shapiro protocol)



  - Achieves optimal rate-loss scaling: within factor of 2-3 of best possible rate (in bits/mode)
  - Shapiro QI wprotocol's bits/mode highly suboptimal. But very high modes/sec due to the naturally broadband SPDC, hence resulting in a higher bits/second than above
- Can we get around this shortcoming of our protocol?

Distribution Statement A. Approved for public release; distribution is unlimited.

High-rate direct-secure comm. using DSSS laser light, homodyne

- Direct sequence spread spectrum (DSSS) CDMA is a way to tap a broad BW
- Our protocol if equipped with a laser transmitter, AWG, and a broadband homodyne detection, will work the same way, but in a DSSS mode. Will achieve MUCH higher secret bits/sec than QI protocol, but with simpler hardware (1 Mbps over 10 dB loss should be possible)
- DSSS is a also popular way to achieve stealth (LPD/covert communication), and anti-jamming capability
- We recently discovered and implemented the quantum limit to covert communication (sqrt(N) bits can be sent both reliably and deniably in N modes)

Boulat A. Bash, Andrei H. Gheorghe, Monika Patel, Jonathan L. Habif, Dennis Goeckel, Don Towsley, and Saikat Guha, "Covert Optical Communication", in review with *Nature* (2014)

Technical update

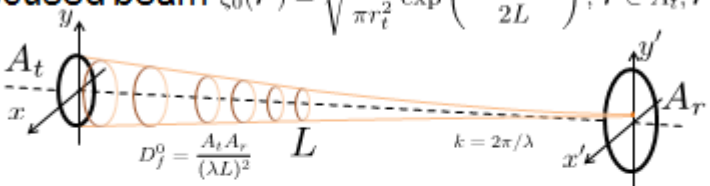
- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

Distribution Statement A. Approved for public release; distribution is unlimited.

Atmospheric LOS turbulent channel: spatial modes

Raytheon BBN Technologies

- Focused beam $\xi_0(\boldsymbol{r}') = \sqrt{\frac{1}{\pi r_t^2}} \exp\left(\frac{-jk|\boldsymbol{r}|^2}{2L}\right)$; $\boldsymbol{r} \in A_t, \boldsymbol{r}' \in A_r$



  - Transmittance, $\eta(t)$ is random process in turbulence

$$\bar{\eta}_G = E[\eta(t)] = \int_0^1 \frac{8\sqrt{D_f^0}}{\pi} e^{-D(2r_t x)/2}\left[\cos^{-1}(x) - x\sqrt{1-x^2}\right] J_1\left(4x\sqrt{D_f^0}\right) dx \qquad D(x) = 1.09\, k^2 C_n^2 L\, x^{5/3}$$

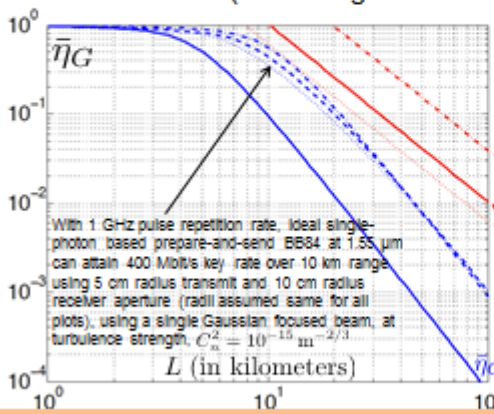
Shapiro, Phys. Rev. A 67, 022309, (2003)

  - Vacuum-prop. channel accommodates infinite orthogonal spatial-mode pairs. Transmittances add up to: $D_f^0 = \sum_{n=1}^{\infty} \eta_n^0$
  - In turbulence, at any time, channel can accommodate infinite mode pairs. Modes, and transmittances are random: $D_f = \sum_{n=1}^{\infty} \eta_n$
    - Far field: one usable spatial mode, with $\eta_1 \approx D_f \ll 1$
    - Near field: $\approx D_f$ unity-transmittance turbulent modes
    - Mean transmittance of fundamental mode in turbulence satisfies the following bounds: $\bar{\eta}_G \le E[\eta_1] \le \min(1, D_f^0)$

Single-mode turbulent channel Mean transmittance of a Gaussian FB

Raytheon BBN Technologies

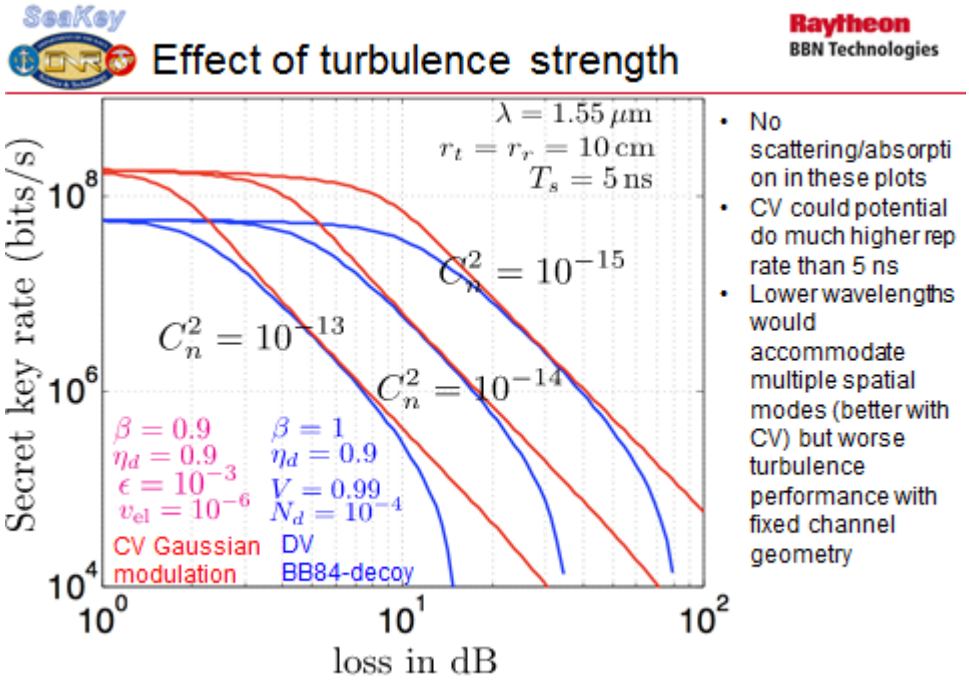
- Mean transmittance of a focused Gaussian beam
  - First-order estimate of SP-BB84 key rate in turbulence, using *one* FB (assuming loss and turbulence as the only



- Propagation at near-far field boundary ($D_f \approx$) at 10s of km range. Multiple spatial modes will help only marginally, unless larger apertures are used. At most 3-4 modes will be useful. Orthogonal spatial modes *not* required. FBs sufficient.

Factors that will decrease key-rate: Employing decoy-state coherent-state BB84, detector excess noise, dark clicks, laser intensity noise, sub-unity coding efficiency, smaller apertures, stronger turbulence
Factors that will boost key rate: Using multiple (few) spatial modes, both polarizations, larger apertures, weaker turbulence, shorter wavelength (will enable more higher-transmittance spatial modes)

Distribution Statement A. Approved for public release; distribution is unlimited.



- No scattering/absorption in these plots
- CV could potential do much higher rep rate than 5 ns
- Lower wavelengths would accommodate multiple spatial modes (better with CV) but worse turbulence performance with fixed channel geometry

Distribution Statement A. Approved for public release; distribution is unlimited.

Technical update

Raytheon BBN Technologies

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

QKD in atmospheric detriments

Raytheon BBN Technologies

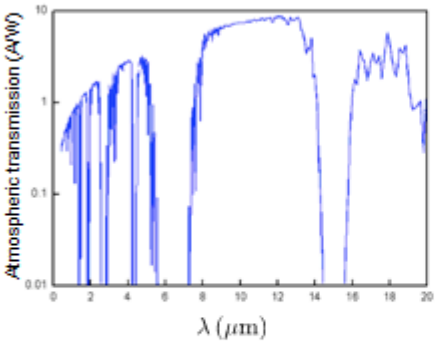
- Narrow down wavelength choices using atmospheric transmission (absorption) data
- Delineate level of detriments at each wavelength
  - Loss: contributions from (1) atmospheric absorption, (2) aerosols, (3) water vapor, (4) turbulence-induced amplitude and phase fluctuations
  - Noise: contributions from thermal

Michael Jack, Raytheon RVS
Monika Patel, Raytheon BBN

- Additional contributions from detector
  - Loss: detection efficiency (DE); Noise: dark clicks (N_d)
  - Different detector type (direct, homodyne) for different protocol, and wavelength of operation, affects DE, N_d

Distribution Statement A. Approved for public release; distribution is unlimited.

Loss (1): Atmospheric absorption



Typical curve of atmospheric transmission in clear weather (detector response considered λ-independent)

H. Manor and S. Arnon, Appl. Optics 42, p. 4285 (2003)

- Why not operate deeper in the infrared?
  - Quantum cascade lasers (QCL) capable of producing weak coherent states between 3.5 μm and 67 μm
  - Problem is availability of single-photon sensitive detector
    - SFG-up-convert to visible and use Si-APD
    - SNSPD (W-Si or other material) responsive in MWIR?

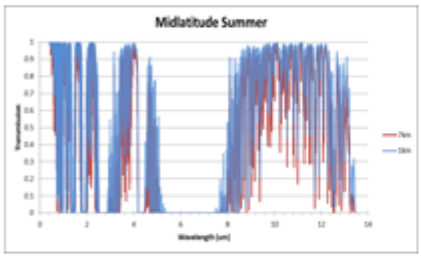
Temporao, Zbinden, Tanzilli, Gisin, Aellen, Giovannini, Faist, der Weid, QIC, No. 1-2 (2008)

Distribution Statement A. Approved for public release; distribution is unlimited.

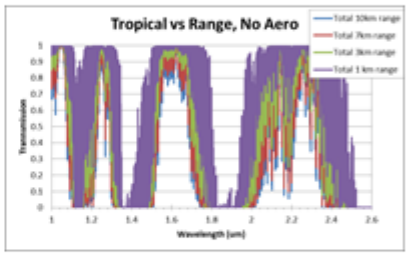
Modeling of absorption

Raytheon BBN Technologies

Mid-latitude Summer, elevation 10m, Ranges of 1 km and 7 km, no aerosol



Tropical atmosphere, elevation 10m, Ranges 1, 3, 7, 10 km, no aerosol



- RVS used MODTRAN (Ontar PcModWin5.2) software to generate atmospheric transmission estimates for MLS (mid-latitude summer) and tropical environments, for a range of distances at elevation 10m above sea level
- The absorption bands due to various elements in the atmosphere (CO_2, H_2O, ozone etc.) result in varying transmission levels
- Candidate good wavelengths, purely from transmission data: 1.55μm, 2.2μm, 4μm

19 5/19/2014

Loss (2): Aerosol contribution

Raytheon BBN Technologies

- Marine aerosol concentrations are in the range of 100 to 300 cm^{-3}
- The size distribution usually contains 3 modes:
  - nucleic D<100 nm
  - accumulation 100<D<600 nm
  - coarse (D>600 nm)

Mode	Material	R_{eff} [μm]	Re(n)	Im(n)
0	Non-hygroscopic dust	0.03	1.52	8×10^{-3}
1	Water soluable + water	0.03	1.37	9.6×10^{-5}
2	Sea salt + water ("aged" aerosol)	0.24	1.38	6.9×10^{-5}
3	Sea salt + water (new aerosol)	2	1.37	6.5×10^{-5}
4	Sea salt + water (near-surface)	8	1.37	6.5×10^{-5}

Table 3: Aerosol material composition, mean radius, and refractive index of the various ANAM aerosol modes for RH = 80%, $U_{10} = U_{24} = 5$ m/sec, AMP = 8, h = 5 m, $\lambda = 1.045\,\mu m$.

Phillip Sprangle, Joseph Penano, NRL, 2005

- Coarse particles makes up 95% mass but only 5% of particle number
- Sea-salt aerosol concentrations in marine boundary layer (MBL)~5-30 cm^{-3}
- Aerosol extinction increases towards sea surface due to greater concentration
- Aerosol transmission generally increases with wavelength in the 2-10 μm wavelength range

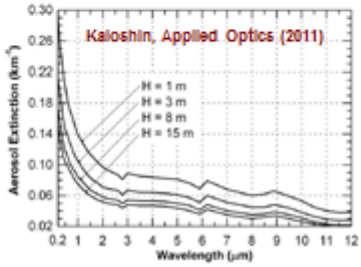
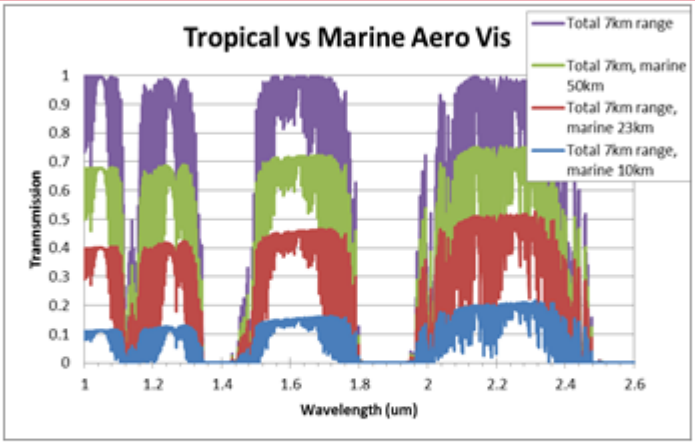


Fig. 6. Aerosol extinction spectra for different values of height above sea level (H).

Distribution Statement A. Approved for public release; distribution is unlimited.

Modeling of aerosol contribution

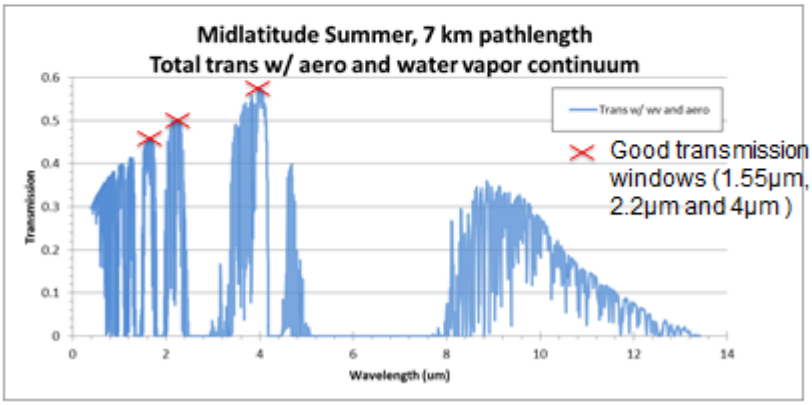


Elevation 10 m from sea level, range = 7 km

- Marine atmospheric transmission data in the presence of aerosol for a few candidate visibilities (10 km, 23 km and 50 km) was generated from the MODTRAN database

Loss (3): Water vapor

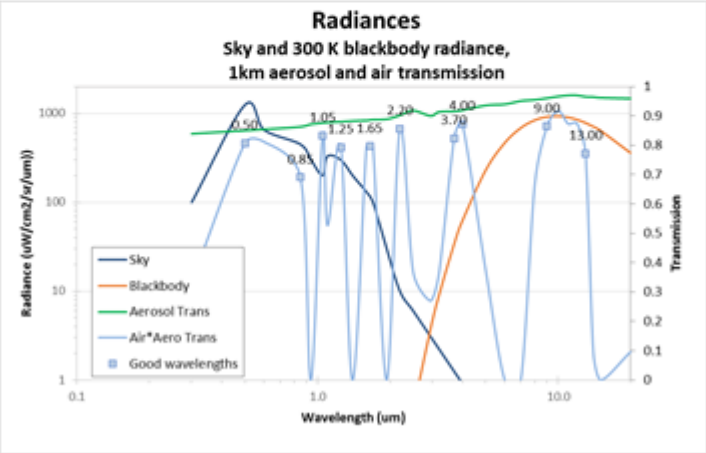
- Combined transmission with all three losses
  - Mid-Latitude Summer, with water vapor, maritime aerosol, 23 km visibility, 7 km range



Distribution Statement A. Approved for public release; distribution is unlimited.

Loss, noise across wavelengths

- Note that of 2.2 μm and 4 μm, former has worse (higher) loss, but better (lower) noise

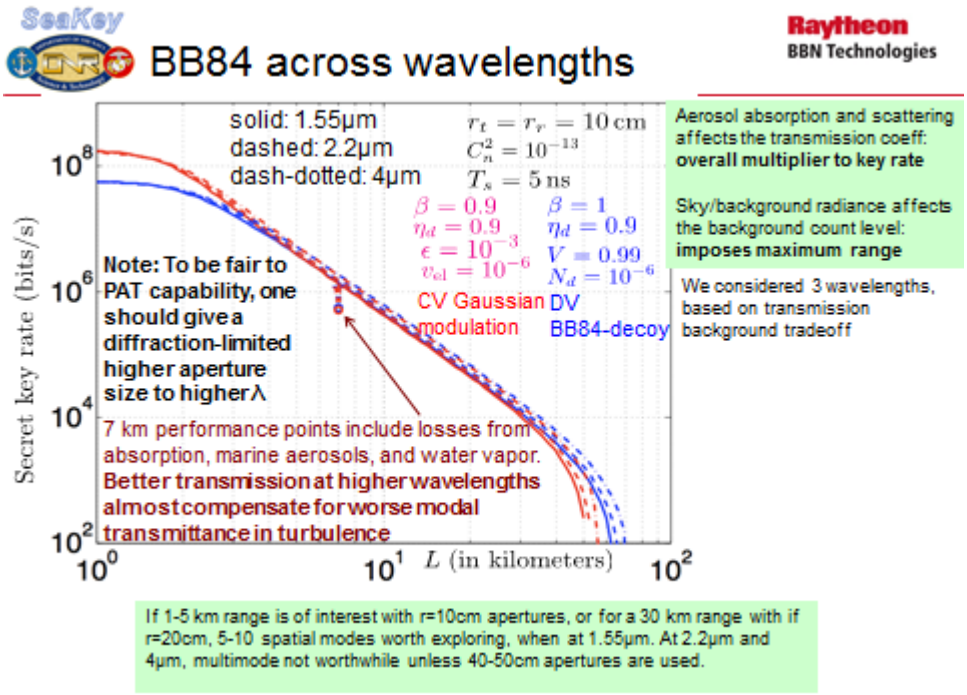


Noise: Background and Sky

- Assumptions for background count calculations
  - Spectral filter width: 1 pm
  - Radius of receiver aperture: 10 cm
  - Field of view of receiver: 5 arc second

Wavelength	Blackbody radiance ($W\ m^{-2}\ sr^{-1}\ \mu m^{-1}$)	Sky radiance ($W\ m^{-2}\ sr^{-1}\ \mu m^{-1}$)	Background counts/sec due to blackbody radiance	Background counts/sec due to sky radiance
1550 nm	0.000000566	1.5	6.4E-05	169.6
2200 nm	0.000839	0.2	0.2	32.3
4000 nm	0.7373	0.009	215.1	2.6

Distribution Statement A. Approved for public release; distribution is unlimited.



Distribution Statement A. Approved for public release; distribution is unlimited.

Technical update

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

Hardware and ancillary technology optimization

Identification of hardware resources for stable free-space transmission

- The NovaSol free-space optical communications interrogator offers position, acquisition and tracking capability at 1.5 μm in a single compact box, and has been tested over a distance of 50 km in a naval environment. This operates in the telecom-band region of 1550 nm and can be modified to implement a free-space qkd channel.

Distribution Statement A. Approved for public release; distribution is unlimited.

Technical update

Raytheon BBN Technologies

- Summary of results
  - Rate vs. loss
  - CV vs. DV
  - Direct secure-communication with laser light
  - Effect of turbulence strength to key rate vs. loss
  - QKD in atmospheric detriments: wavelength comparison
  - Hardware and ancillary technology optimization
  - Full numerical model to get "partials" to key rate w.r.t. each tunable parameter in the end-to-end system

Numerical model

Raytheon BBN Technologies

Seakey Year 1 goals:

- Identify challenges unique to marine deployment, rate-distance tradeoffs with turbulence, scattering, absorption, background, PAT error (e.g., due to platform fluctuations).
- Optimize performance across choice of protocol, code, modulation, wavelength, transmitter-receiver technology.

In order to address these goals, we have built a numerical model which generates the secret key rate (in bits/sec) for the following QKD protocols:

- DV BB84 with laser decoy
- CV with Gaussian modulation

This numerical model incorporates following user-defined values:

- Wavelength
- Geographical zone (eg. Tropical, Mid-latitude etc.)
- Weather conditions (eg. clear, cloudy, raining)
- Visibility (corresponding to a specific aerosol contribution)
- Elevation above sea-level

These values are drawn from the MODTRAN database, which is an extensively validated atmospheric radiative transfer model, accessed by the Ontar PcModWin 5.2 software.

The model draws the transmission coefficient from the MODTRAN database.

INPUT

- *QKD protocol*
- *Conditions such as geographical location, range etc.*

Get "partials" (sensitivity to a parameter at an operating point)

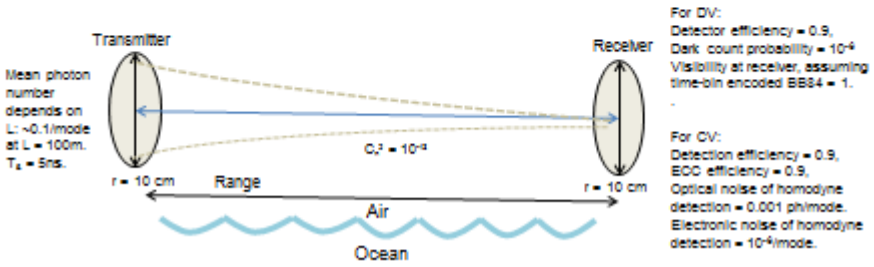
OUTPUT

The expected secret key rate (in bits/mode) as drawn from expected values of transmission, background etc. for the chosen conditions.

Distribution Statement A. Approved for public release; distribution is unlimited.

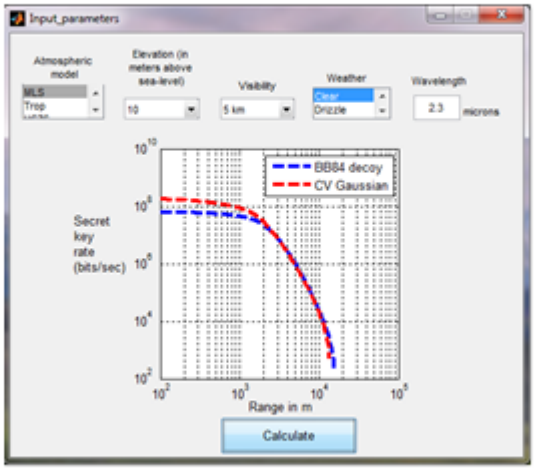
Instructions:

- Download model.zip.
- At the command prompt in Matlab, type 'Input_parameters'. This will run the m-code which produces a GUI for the user to enter choice of wavelength, weather condition etc.
- The file 'Input_parameters' models the case of a single spatial mode and takes turbulence into account. A second m-file, "Input_parameters_multimodes' models multiple spatial modes in a soft-aperture configuration, and does not include the effects of turbulence.
- The following link geometry is modeled:



Distribution Statement A. Approved for public release; distribution is unlimited.

Screenshot of Matlab GUI



Taking multiple spatial modes into account

- Free-space propagation:
  - Far field, $D_f = \frac{A_t A_r}{(\lambda L)^2} \ll 1$
    - One spatial mode ($\eta \approx D_f$) has any appreciable transmittance
    - Rate, $R \sim 1/L^2$
  - Near field, $D_f \gg 1$
    - There are $M \approx D_f$ unit-transmittance spatial modes, i.e., $\eta_m \approx 1$
    - Rate, $R \sim 1/L^2$
    - Secret key rate = $R(\eta_1) + 2R(\eta_2) + ... + MR(\eta_M)$
- If we consider Hermite-Gaussian and Laguerre-Gaussian modes in a soft-aperture configuration, their modal transmissivities are given by:

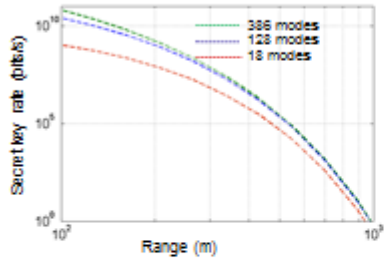
$$\eta_m = \left(\frac{1 + 2D_f - \sqrt{1 + 4D_f}}{2D_f} \right)^m$$

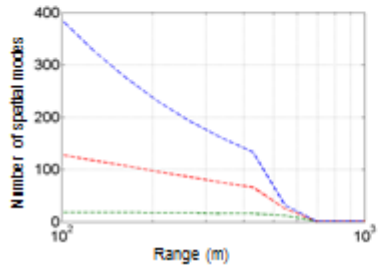
Here, $D_f = \left(kr_T^2/4L\right)\left(kr_R^2/4L\right)$ is the product of the transmitter-pupil and receiver-pupil Fresnel numbers in a soft-aperture configuration. There are m spatial modes with transmitivitty η_m .

Distribution Statement A. Approved for public release; distribution is unlimited.

Taking multiple spatial modes into account … contd.

Raytheon BBN Technologies





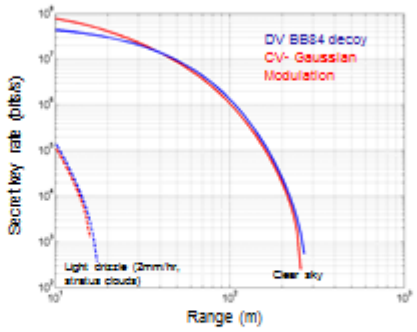
- The adjacent figure depicts the dependence of the secret key rate of the BB84-decoy state protocol when multiple spatial modes are taken into account. As expected, this is more pronounced at shorter ranges.
- The calculation uses a series of increasing mode numbers until the condition $MR(\eta_M)/R_{tot} < 0.1$ is satisfied.
- The rate advantage at low range is at the cost of many spatial modes.

A few examples

Raytheon BBN Technologies

Solid lines: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 1550nm wavelength

Dashed lines: Mid-Latitude Summer, light drizzle, 0m above sea-level, aerosol visibility: 50km, 1550nm wavelength



Transmission quickly drops in cloudy and rainy weather (from η = 0.96 to η = 0.5463 and η = 0.16 for light and heavy rain respectively, leading to a rapid decrease in key rates.)

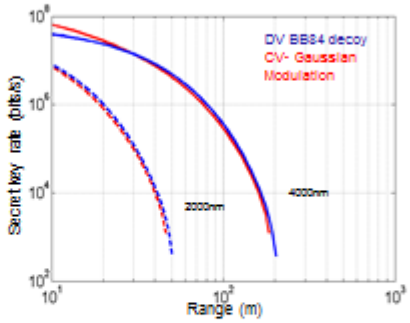
Distribution Statement A. Approved for public release; distribution is unlimited.

A few examples … contd.

Raytheon BBN Technologies

Solid lines: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 2000nm wavelength

Dashed lines: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50km, 4000nm wavelength



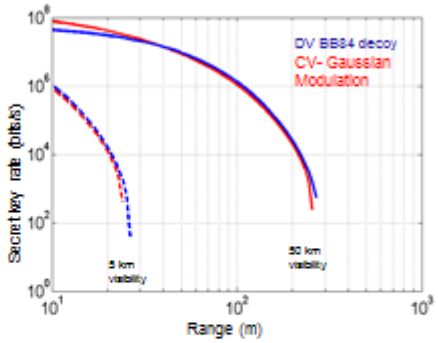
Taking only transmission into account, the rates for operation at 2000nm are smaller than those at 4000nm. Not included in this model is the difference in detection efficiencies and background count rates due to sky radiance and blackbody radiance.

A few examples … contd.

Raytheon BBN Technologies

Solid lines: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 1550nm wavelength

Dashed lines: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 5km, 1550nm wavelength



50 km visibility is relatively high for coastal environments, and this only occurs on very clear days[1]. If the visibility drops to 5 km, the key rate decreases rapidly as shown.

[1]Visibility measurements along extended paths over the ocean surface, J. E. Shields et al, Proc. of SPIE Vol. 5891.

Distribution Statement A. Approved for public release; distribution is unlimited.

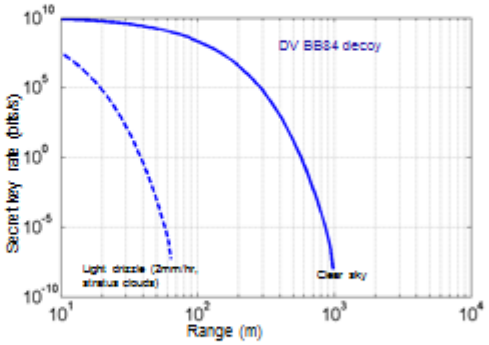
A few examples … contd.

Raytheon BBN Technologies

Including multiple spatial modes (no turbulence):

Solid line: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 1550nm wavelength

Dashed line: Mid-Latitude Summer, light drizzle, 0m above sea-level, aerosol visibility: 50km, 1550nm wavelength



Access to multiple spatial modes at low ranges results in an increase of two orders of magnitude in key rate.

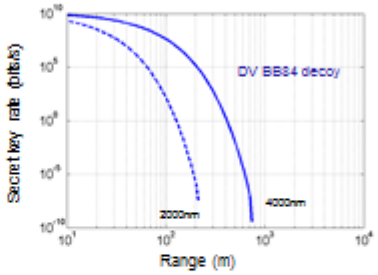
A few examples … contd.

Raytheon BBN Technologies

Including multiple spatial modes (no turbulence):

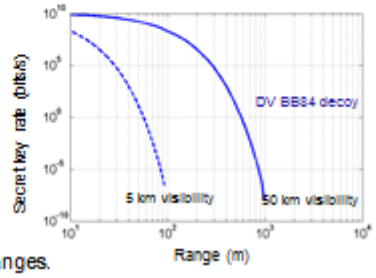
Solid line: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 4000nm wavelength

Dashed line: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50km, 2000nm wavelength



Solid line: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 50 km, 1550nm wavelength

Dashed line: Mid-Latitude Summer, clear sky, 0m above sea-level, aerosol visibility: 5km, 1550nm wavelength



This incorporates 19 spatial modes at low ranges.

Distribution Statement A. Approved for public release; distribution is unlimited.

In conclusion

Raytheon
BBN Technologies

- With losses from aerosol scattering, water vapor continuum absorption and turbulence, and realistic noise levels at the detectors, the secret key rates of the CV-Gaussian and DV BB84 decoy protocols drop rapidly beyond a range of 100-1000 meters.

- For the lower ranges, the ability to "turn on" multi-spatial-mode operation, and choose up to a certain number of spatial modes, helps in increasing key rates by a few orders of magnitude.

- It may be more realistic to assume that only a fraction of the photons not collected by Bob, are received by Eve. We will incorporate this correction in a future version of the numerical model.

Distribution Statement A. Approved for public release; distribution is unlimited.